BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11252111 A**

(43) Date of publication of application: **17 . 09 . 99**

(51) Int. Cl **H04L 12/28**
H04Q 3/00

(21) Application number: **10053677**

(22) Date of filing: **05 . 03 . 98**

(71) Applicant: **KDD CORP**

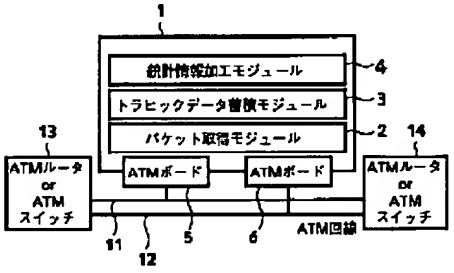
(72) Inventor: **OGISHI TOMOHIKO**
IDOGAMI AKIRA
KATO SATOHIKO

(54) TRAFFIC MONITOR DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To compress and store traffic data in a way as close as to that of packets set through a channel for the Internet or the like.

SOLUTION: The traffic monitor device uses a packet acquisition module 2 to extract a packet through asynchronous transfer mode ATM lines 1, 12 of the Internet and to extract a header part including an IP header, which is given to a traffic data storage module 3. Then the module 3 checks an outgoing/incoming network ID NID of the packet and a higher-ranking protocol of the IP from the header part, records the traffic data in a preset format based on the combination between the outgoing/incoming network ID and the higher-ranking protocol according to a preset format and stores the traffic data for each prescribed time while collecting the data of the same kind of the combination. Furthermore, the traffic data storage module 3 stores the traffic data having already been stored for the same kind while collecting the data for each same kind for each prescribed longer time.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－252111

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/20	Ｇ
Ｈ０４Ｑ　3/00		Ｈ０４Ｑ　3/00	

審査請求　未請求　請求項の数12　ＯＬ　（全７頁）

(21)出願番号　特願平10－53677

(22)出願日　平成10年(1998)３月５日

(71)出願人　000001214
ケイディディ株式会社
東京都新宿区西新宿２丁目３番２号

(72)発明者　大岸　智彦
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　井戸上　彰
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

(72)発明者　加藤　聰彦
東京都新宿区西新宿二丁目３番２号　国際電信電話株式会社内

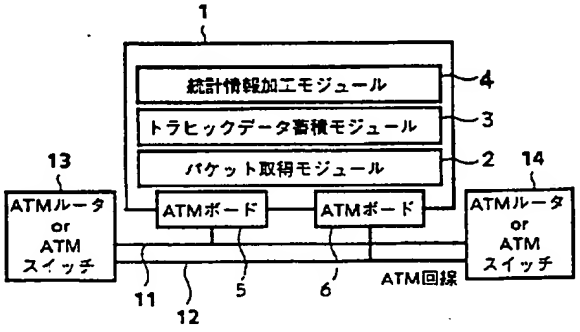
(74)代理人　弁理士　光石　俊郎　（外２名）

(54)【発明の名称】　トラヒック監視装置

(57)【要約】

【課題】　インターネット等の回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積すること。

【解決手段】　パケット取得モジュール２によりインターネットのＡＴＭ回線１、１２からパケットを抽出してＩＰヘッダを含むヘッダ部分を取り出し、トラヒックデータ蓄積モジュール３に渡す。モジュール３はヘッダ部分からパケットの発着ＮＩＤとＩＰの上位プロトコルを調べ、発着ＮＩＤと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上記組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積する。更に、トラヒックデータ蓄積モジュール３により、既に同一種類毎にまとめて蓄積されたトラヒックデータ同士を、より長い一定時間毎に、同一種類毎にまとめて蓄積する。



1

【特許請求の範囲】

【請求項１】　ネットワーク間回線からパケットを抽出し、抽出したパケットの少なくともＩＰヘッダを含むヘッダ部分を取り出すパケット取得手段と、前記パケット取得手段が取り出したヘッダ部分の内容から同パケット取得手段が抽出したパケットのパケット発信側ネットワークＩＤ及びパケット着信側ネットワークＩＤとの組み合わせ（以下、発着ＮＩＤと呼ぶ）を調べ、発着ＮＩＤ別に、前記回線上のトラヒックに関するデータ（以下、トラヒックデータと呼ぶ）を予め設定されたフォーマットで記録し、一定時間毎に発着ＮＩＤが同一種類のトラヒックデータ同士をまとめて蓄積するトラヒックデータ蓄積手段を備えることを特徴とするトラヒック監視装置。

【請求項２】　前記トラヒックデータ蓄積手段は、発着ＮＩＤに加えて、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットのＩＰプロトコルよりも上位のプロトコル（以下、上位プロトコルと呼ぶ）を調べ、発着ＮＩＤと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に発着ＮＩＤと上位プロトコルの組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とする請求項１に記載のトラヒック監視装置。

【請求項３】　前記トラヒックデータ蓄積手段は、発着ＮＩＤの代わりに、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットの上位プロトコルを調べ、上位プロトコル別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上位プロトコルが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とする請求項１に記載のトラヒック監視装置。

【請求項４】　前記上位プロトコルはＴＣＰプロトコル、ＵＤＰプロトコル、ＨＴＴＰプロトコル、ＦＴＰプロトコル及びＳＭＴＰプロトコルのうち少なくとも１つであることを特徴とする請求項２又は３に記載のトラヒック監視装置。

【請求項５】　前記トラヒックデータ蓄積手段は、前記同一種類毎にまとめて蓄積されたトラヒックデータ同士を、更に、前記一定時間より長い他の一定時間毎に、同一種類毎にまとめて蓄積することを特徴とする請求項１から４いずれかに記載のトラヒック監視装置。

【請求項６】　前記トラヒックデータとして、ＩＰプロトコルに関する情報（以下、ＩＰ情報と呼ぶ）、ＴＣＰプロトコルに関する情報（以下、ＴＣＰ情報と呼ぶ）、ＵＤＰプロトコルに関する情報（以下、ＵＤＰ情報と呼ぶ）及びアプリケーションプロトコルに関する情報（以下、アプリケーションプロトコル情報と呼ぶ）のうち少なくとも１種類を含むことを特徴とする請求項１から５いずれかに記載のトラヒック監視装置。

2

【請求項７】　前記ＩＰ情報として、少なくともＩＰパケット総数及びＩＰパケット総バイト数を含むことを特徴とする請求項６に記載のトラヒック監視装置。

【請求項８】　前記ＴＣＰ情報がコネクションに関しないＴＣＰ情報とコネクションに関するＴＣＰ情報とに区別されること特徴とする請求項６に記載のトラヒック監視装置。

【請求項９】　前記コネクションに関しないＴＣＰ情報として少なくともＴＣＰセグメント総数及びＴＣＰセグメント総バイト数を含むことを特徴とする請求項８に記載のトラヒック監視装置。

【請求項１０】　前記コネクションに関するＴＣＰ情報として少なくともコネクション数を含むことを特徴とする請求項８に記載のトラヒック監視装置。

【請求項１１】　前記ＵＤＰ情報として少なくともＵＤＰデータグラム総数及びＵＤＰデータグラム総バイト数を含むことを特徴とする請求項６に記載のトラヒック監視装置。

【請求項１２】　前記アプリケーションプロトコル情報として、ＨＴＴＰプロトコルに関する情報、ＦＴＰプロトコルに関する情報及びＳＭＴＰプロトコルに関する情報のうち少なくとも１つを含むことを特徴とする請求項６に記載のトラヒック監視装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はインターネット等、ネットワーク間のパフォーマンス解析に有用なトラヒック監視装置に関する。

【０００２】

【従来の技術】インターネットの普及に伴い、特定の回線を流れるトラヒックの時間的変化など、インターネットのパフォーマンス解析が重要な課題となっている。

【０００３】このようなパフォーマンス解析を行うには、回線を流れるトラヒックを長時間監視して、それに基づいて各種の統計情報を生成する必要がある。

【０００４】一方、トラヒックの増大に伴い、インターネットのバックボーン回線はＡＴＭ（非同期転送モード：Asynchronous Transfer Mode）回線などの使用により、高速化されてきている。

【０００５】しかし、回線上に流れるパケットを加工せずに使用すると、時間に比例してデータ量が増大する。従って、ＡＴＭ回線のような高速ネットワークに対してトラヒックを長時間監視する場合は、トラヒックデータの量が極めて膨大なものとなる。そのため、大容量の記憶装置と高速な処理装置が必要になる。

【０００６】

【発明が解決しようとする課題】そこで本発明の課題は、回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積するトラヒック監視装置を提供することである。

3

【０００７】

【課題を解決するための手段】上記課題を解決する請求項１に係る発明は、ネットワーク間回線からパケットを抽出し、抽出したパケットの少なくともＩＰヘッダを含むヘッダ部分を取り出すパケット取得手段と、前記パケット取得手段が取り出したヘッダ部分の内容から同パケット取得手段が抽出したパケットのパケット発信側ネットワークＩＤ及びパケット着信側ネットワークＩＤとの組み合わせ（以下、発着ＮＩＤと呼ぶ）を調べ、発着ＮＩＤ別に、前記回線上のトラヒックに関するデータ（以下、トラヒックデータと呼ぶ）を予め設定されたフォーマットで記録し、一定時間毎に発着ＮＩＤが同一種類のトラヒックデータ同士をまとめて蓄積するトラヒックデータ蓄積手段を備えることを特徴とするトラヒック監視装置である。

【０００８】また、請求項２に係る発明は、前記トラヒックデータ蓄積手段が、発着ＮＩＤに加えて、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットのＩＰプロトコルよりも上位のプロトコル（以下、上位プロトコルと呼ぶ）を調べ、発着ＮＩＤと上位プロトコルの組み合わせ別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に発着ＮＩＤと上位プロトコルの組み合わせが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とするトラヒック監視装置である。

【０００９】請求項３に係る発明は、前記トラヒックデータ蓄積手段が、発着ＮＩＤの代わりに、パケット取得手段が取り出した前記ヘッダ部分の内容から同パケット取得手段が抽出したパケットの上位プロトコルを調べ、上位プロトコル別に、トラヒックデータを予め設定されたフォーマットで記録し、一定時間毎に上位プロトコルが同一種類のトラヒックデータ同士をまとめて蓄積することを特徴とするトラヒック監視装置である。

【００１０】請求項４に係る発明は、前記上位プロトコルがＴＣＰプロトコル、ＵＤＰプロトコル、ＨＴＴＰプロトコル、ＦＴＰプロトコル及びＳＭＴＰプロトコルのうち少なくとも１つであることを特徴とするトラヒック監視装置である。

【００１１】請求項５に係る発明は、前記トラヒックデータ蓄積手段が、前記同一種類毎にまとめて蓄積されたトラヒックデータ同士を、更に、前記一定時間より長い他の一定時間毎に、同一種類毎にまとめて蓄積することを特徴とするトラヒック監視装置である。

【００１２】請求項６に係る発明は、前記トラヒックデータとして、ＩＰプロトコルに関する情報（以下、ＩＰ情報と呼ぶ）、ＴＣＰプロトコルに関する情報（以下、ＴＣＰ情報と呼ぶ）、ＵＤＰプロトコルに関する情報（以下、ＵＤＰ情報と呼ぶ）及びアプリケーションプロトコルに関する情報（以下、アプリケーションプロトコル情報と呼ぶ）のうち少なくとも１種類を含むことを特

4

徴とするトラヒック監視装置である。

【００１３】請求項７に係る発明は、前記ＩＰ情報として少なくともＩＰパケット総数及びＩＰパケット総バイト数を含むことを特徴とするトラヒック監視装置である。

【００１４】請求項８に係る発明は、前記ＴＣＰ情報がコネクションに関しないＴＣＰ情報とコネクションに関するＴＣＰ情報とに区別されること特徴とするトラヒック監視装置である。

【００１５】請求項９に係る発明は、前記コネクションに関しないＴＣＰ情報として少なくともＴＣＰセグメント総数及びＴＣＰセグメント総バイト数を含むことを特徴とするトラヒック監視装置である。

【００１６】請求項１０に係る発明は、前記コネクションに関するＴＣＰ情報として少なくともコネクション数を含むことを特徴とするトラヒック監視装置である。

【００１７】請求項１１に係る発明は、前記ＵＤＰ情報として少なくともＵＤＰデータグラム総数及びＵＤＰデータグラム総バイト数を含むことを特徴とするトラヒック監視装置である。

【００１８】請求項１２に係る発明は、前記アプリケーションプロトコル情報として、ＨＴＴＰプロトコルに関する情報、ＦＴＰプロトコルに関する情報及びＳＭＴＰプロトコルに関する情報のうち少なくとも１つを含むことを特徴とするトラヒック監視装置である。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態を説明する。

【００２０】（トラック監視装置の設計方針）本発明の実施の形態の係るトラック監視装置の設計にあたり、以下の方針を立てた。

（１）一定時間毎（例えば、１０分毎）に。ＩＰ、ＴＣＰ、ＨＴＴＰ、ＦＴＰ及びＳＭＴＰ（Simple Mail Transfer Protocol：シンプルメール転送プロトコル）等の各プロトコルの統計情報を生成し、その時間的変化を解析可能とする。これらの情報は、発着ネットワークＩＤ及びアプリケーション毎に生成する。ＴＣＰでは、コネクションの確立時間や再送回数等、通信手順を考慮した情報も対象とする。

（２）インターネットのＡＴＭ回線上を流れるＩＰパケットを取得し、一定時間のトラヒック量等を、トラヒックデータとして蓄積する。統計情報は、このデータを元に生成する。

（３）数カ月分のトラヒックデータを蓄積することを想定し、過去のデータは圧縮することが可能であるようなデータ構造を採用する。

【００２１】（機能）本トラヒック監視装置には、特に、次のような統計情報を生成する機能を持たせた。

【００２２】ＩＰ情報については、

（１）ＡＴＭ回線を流れる総パケット数及び総バイト数

5

（２）発着のネットワークＩＤ毎のパケット数及びバイト数
（３）上位のプロトコルの種別毎のパケット数及びバイト数
等である。

【００２３】ＴＣＰ情報については、
（１）確立されたコネクション数
（２）コネクションの平均接続時間
（３）コネクション当たりの平均再送パケット数
（４）コネクション当たりの平均再送バイト数
等である。

【００２４】ＨＴＴＰ情報については、頻繁にアクセスされるサイト名等である。

【００２５】（装置構成）本トラヒック監視装置は主として、ＣＰＵとソフトウェアを用いた計算機で図１に示すように構成した。但し、計算機はその能力に応じて、１台又は２台以上用いる。。

【００２６】図１に示すトラヒック監視装置１は１５５Ｍｂｐｓの第１のＡＴＭ回線１１及び第２のＡＴＭ回線１２に接続され、その上を流れる双方向のパケットを取得するように構成する。

【００２７】また、図１に示すようにトラヒック監視装置１は、ソフトウェアにより、ＵＮＩＸカーネル内に実装されるパケット取得モジュール（パケット取得手段）２と、ユーザプログラムとして実行されるトラヒックデータ蓄積モジュール（トラヒックデータ蓄積手段）３に加えて、データ集計及び画面表示を行う統計情報加工モジュール４から構成する。

【００２８】更に、トラヒック監視装置１は、第１のＡＴＭ回線１１に接続するためのＡＴＭボード５と、第２のＡＴＭ回線１２に接続するためのＡＴＭボード６を備えている。図１中、１３及び１４はＡＴＭ回線に接続される各ネットワークのＡＴＭルータまたはＡＴＭスイッチを示す。

【００２９】（各モジュールについて）パケット取得モジュール２では、ＩＰパケットのキャプチャを行い、ＩＰ、ＴＣＰ、ＨＴＴＰ等のヘッダ部分を取り出し、トラヒックデータ蓄積モジュール３へ通知する。

【００３０】トラヒックデータ蓄積モジュール３では、通知されたパケット情報を元に、一定時間毎にトラヒックデータを作成し、圧縮して蓄積する。

【００３１】図４に、トラヒックデータのフォーマット例を示す。例えば、トラヒックデータは、一定時間内にキャプチャされた、発着ネットワークＩＤ（発着ＮＩＤ：発ＮＩＤと着ＮＩＤ））及び発着ポート(well-known ポート：発側ポート番号と着側ポート番号）が同一であるＩＰパケットに対して作成され、前述の統計情報を作成するための情報を保持する。

【００３２】このように一定時間内に転送された複数のＩＰパケットに対応する情報を圧縮して蓄積することにより、ヘッダ部分を個別に識別する場合に比べて、蓄積すべきデータ量を減少させることができると共に、過去の記録については統計情報の生成の時間間隔を長くすることにより、データの圧縮が可能である。

【００３３】統計情報加工モジュール４は、蓄積されたトラヒックデータの集計及び画面表示を行う。これにより、或るネットワークＩＤが過去１ヶ月間にＦＴＰにより受信したデータの総バイト数や、或るＦＴＰサーバがＴＣＰのコネクション確立に失敗した回数の１週間の分布など、詳細な統計情報を生成することができる。

【００３４】本トラヒック監視装置１は、パケット情報を圧縮、加工して蓄積することにより、高速なインターネットに対応して長時間運用することができる。

【００３５】（トラヒック監視装置１の実施例）以下、図２及び図３に基づいて、トラヒック監視装置１の具体的な実施例を説明する。

【００３６】（パケット取得モジュール２の詳細）先ず、図２を参照して、パケット取得モジュール２の詳細なパケット取得処理手順を以下に説明する。

【００３７】パケット取得モジュール２はＡＴＭボード５、６を通してＡＴＭ回線１１、１２を監視し、ＡＴＭ回線１１、１２からそこに流れるパケットを抽出してする（図２のステップＳ１参照）。

【００３８】次に、パケット取得モジュール２は、取得したパケットからそのヘッダ部分のみを取り出す（ステップＳ２参照）。詳しくは、パケットのヘッダ部分からＩＰ（インターネットプロトコル）の上位プロトコルを調べる。上位プロトコルがＴＣＰ（転送制御プロトコル：Transmission Control Protocol ）及びＵＤＰ（ユーザデータグラムプロトコル：User Datagram Protocol）以外である場合は、ＩＰヘッダのみを取り出す。上位プロトコルがＴＣＰ又はＵＤＰである場合は、ＴＣＰ又はＵＤＰのポート番号から更に上位のアプリケーションプロトコルを調べ、アプリケーションプロトコル毎にそのフォーマットを解析して、アプリケーションプロトコルのヘッダ部分までを取り出す。

【００３９】パケット取得モジュール２は、上記のように取り出したＩＰヘッダ及びアプリケーションプロトコルのヘッダ部分をトラヒックデータ蓄積モジュール３へ渡す（ステップＳ３参照）。

【００４０】（トラヒックデータ蓄積モジュール３の詳細）次に、図３を参照して、トラヒックデータ蓄積モジュール３の詳細なトラヒックデータ蓄積手順を以下に説明する。

【００４１】トラヒックデータ蓄積モジュール３は常時、データの圧縮を行うべき一定時間が経過したか否かを監視する（図３のステップＳ４参照）。

【００４２】一定時間が経過しない場合は、その間、パケット取得モジュール２から渡されたデータ（ＩＰヘッダ又はアプリケーションプロトコルのヘッダ部分）があ

るか否かを調べる（ステップＳ５参照）。

【００４３】パケット取得モジュール２からデータが渡されていた場合は、そのデータに対応するトラヒックデータが既に存在しているか否かを調べ、そのトラヒックデータのＩＤを取得する（ステップＳ６参照）。詳しくは、パケット取得モジュール２から渡されたヘッダ部分から、パケット取得モジュール２が抽出したパケットの発着ＮＩＤ（発着ネットワークＩＤ）と発着ポート番号を調べることにより、対応するトラヒックデータを検出し、そのＩＤを取得する。対応するトラヒックデータが存在していない場合は、新規にＩＤを付して作成する。

【００４４】トラヒックデータのフォーマットとしては、発着ＮＩＤ及び発着ポートが同一であるＩＰパケットに対して作成され、大まかには、図４に符号７で示すように、ＩＰ情報、ＴＣＰ情報又はＵＤＰ情報、並びに、ＨＴＴＰ情報という４種類の情報を記録対象とするようにしてある。

【００４５】まず、トラヒックデータ蓄積モジュール３は、ＩＰ情報を記録する（ステップＳ７参照）。

【００４６】ＩＰ情報の詳細としては、下記（１）～（６）の情報を蓄積するものとしている。

（１）ＩＰパケット総数

（２）ＩＰパケット総バイト数

（３）パケット長の分布

（４）ＩＰフラグメンテーション（ＩＰデータグラムをカプセル化する際にサイズが最大転送単位を越えた場合に分割されたＩＰパケット）を含むＩＰパケット総数

（５）プロトコルＩＤ毎のＩＰパケット総数

（６）プロトコルＩＤ毎のＩＰパケット総バイト数

【００４７】次に、パケット取得モジュール２から渡されたヘッダ部分から、ＩＰの上位プロトコルがＴＣＰ、ＵＤＰ、それ以外（ＩＣＭＰ（インターネット制御メッセージプロトコル：Internet Control Message Protocol）やＩＧＭＰ（インターネットグループ管理プロトコル：Internet Group Management Protocol）等）のいずれであるかを調べ、それぞれの場合について、後述のように別個の処理を行う（ステップＳ８参照）。

【００４８】ＩＰの上位プロトコルがＴＣＰの場合は、まず、コネクションに関しないＴＣＰ情報を記録する（ステップＳ９参照）。

【００４９】コネクションに関しないＴＣＰ情報の詳細としては、下記（１）～（８）の情報を蓄積するものとしている。ここで、双方向とは、サーバ側（ポート番号でアプリケーションを識別する側）からの送信と、クライアント側からの送信とを区別することを意味する。ＴＣＰセグメントのタイプとしては、ＳＹＮ、ＳＹＮ＋ＡＣＫ、ＤＴ（データセグメント）、ＡＣＫ、ＦＩＮ（データあり）、ＦＩＮ（データ無し）、ＲＳＴ、これら以外の異常タイプの８つに区別する。

（１）ＴＣＰセグメント総数（双方向）

（２）ＴＣＰセグメント総バイト数（双方向）

（３）ＭＳＳ（最大セグメントサイズ：Maximum Segment Size）オプションを含むＴＣＰセグメント総数（双方向）

（４）ＷＳＦ（ウインドウスケールファクタ：Window Scale Factor）オプションを含むＴＣＰセグメント総数（双方向）

（５）タイムスタンプ（Time Stamp）オプションを含むＴＣＰセグメント総数（双方向）

（６）再送ＴＣＰセグメント数

（７）タイプ別のＴＣＰセグメント総数（双方向）

（８）タイプ別のＴＣＰセグメント総バイト数（双方向）

【００５０】次に、トラヒックデータ蓄積モジュール３は、ＴＣＰコネクションのＩＤを取得する（ステップＳ１０参照）。詳細には、トラヒックデータ蓄積モジュール３はコネクション管理テーブルと状態遷移機能を備えており、抽出したパケットのＴＣＰ／ＩＰヘッダから発着のＩＰアドレス及び発着のポート番号を抽出することにより、そのパケットのＴＣＰコネクションを識別し、コネクション管理テーブルのリストから、同ＴＣＰコネクションのＩＤを取得する。識別したＴＣＰコネクションがコネクション管理テーブルのリストにない場合は、当該ＴＣＰコネクションをコネクション管理テーブルに追加して新規に作成し、それのＩＤを取得する。

【００５１】そして、トラヒックデータ蓄積モジュール３は、状態遷移及びコネクション管理テーブルの更新をを行う（ステップＳ１１参照）。詳細には、先に取得したＴＣＰコネクションに対して、抽出したパケットのＴＣＰヘッダを入力として与えることにより、状態遷移を行う。ＴＣＰの状態としては、CLOSED（コネクションなし）、SYN_SENT(SYN送信済み)、ESTABLISHED(データ転送中)、INIT_FIN_SENT(FIN送信済み)及びRES _FIN _SENT（FIN 受信済み）の５種類を識別するものとしている。

【００５２】次に、トラヒックデータ蓄積モジュール３は、コネクションに関するＴＣＰ情報を蓄積する（ステップＳ１２参照）。詳細には、先の状態遷移において得られるＴＣＰ情報の蓄積を行う。

【００５３】コネクションに関するＴＣＰ情報としては、下記（１）～（６）の情報を蓄積するものとしている。ここでも、双方向とは、サーバ側からの送信と、クライアント側からの送信とを区別することを意味する。

（１）ＴＣＰコネクション確立成功数

（２）ＴＣＰコネクション確立失敗数

（３）ＴＣＰコネクション確立平均時間

（４）ＴＣＰコネクション持続平均時間

（５）ＴＣＰコネクション毎の平均データ転送量（双方向）

（６）ＴＣＰコネクション毎のスループット（双方向）

9

【００５４】次に、トラヒックデータ蓄積モジュール３は、ＴＣＰの上位プロトコル（アプリケーションプロトコル）を調べる（ステップＳ１３参照）。詳細には、ポート番号よりアプリケーションプロトコルを識別して、そのアプリケーション固有の情報解析を行う。

【００５５】そして、ＴＣＰ上のアプリケーションプロトコル毎に、そのアプリケーション固有の情報の蓄積を行う（ステップＳ１４参照）。例えば、上位アプリケーションプロトコルがＨＴＴＰ(Hyper Text Transfer Protocol:ハイパーテキスト転送プロトコル）であるならば、サイト毎のアクセス数などを蓄積する。

【００５６】ＴＣＰ上のアプリケーション固有の情報を蓄積したら、一定時間経過監視の処理（ステップＳ４）に戻る。

【００５７】一方、ＩＰの上位プロトコルの判定（ステップＳ８）において上位プロトコルがＵＤＰの場合は、ＪＤＰ情報を蓄積する（ステップＳ１５参照）。

【００５８】ＵＤＰ情報としては下記（１）～（２）の情報を蓄積するものとしている。

（１）ＵＤＰデータグラム総数（双方向）

（２）ＵＤＰデータグラム総バイト数（双方向）

【００５９】更に、トラヒックデータ蓄積モジュール３は、ＵＤＰ上のアプリケーションプロトコルをポート番号より識別してそのアプリケーション固有の情報を解析し、得られたアプリケーション固有の情報の蓄積を行う（ステップＳ１６参照）。

【００６０】ＵＤＰ上のアプリケーション固有の情報を蓄積したら、一定時間経過監視処理（ステップＳ４）に戻る。

【００６１】ＩＰの上位プロトコルの判定（ステップＳ８）において上位プロトコルがＴＣＰでも、ＵＤＰでもない場合は、一定時間経過監視の処理（ステップＳ４）に戻る。

【００６２】そして、圧縮すべき一定時間が経過した時、過去のトラヒックデータを、粒度の粗いトラヒックデータに圧縮して変換する（ステップＳ１７参照）。

【００６３】圧縮としては、発着ＮＩＤが同一種類のトラヒックデータ同士をまとめたり、発着ＮＩＤと上位プロトコル（アプリケーションプロトコルであっても良い）が同一種類のトラヒックデータ同士をまとめたり、上位プロトコル（アプリケーションプロトコルであっても良い）が同一種類のトラヒックデータ同士をまとめて蓄積することにより、達成できる。

10

【００６４】同一種類毎にまとめて圧縮されたトラヒックデータ同士を、より長い一定時間毎に、更に同一種類毎にまとめて圧縮して蓄積することにより、粒度がより粗いトラヒックデータに圧縮しても良い。もちろん、必要に応じて何段階にも時間間隔を長くして次々に粒度が粗いトラヒックデータに圧縮しても良い。

【００６５】上記説明では、トラヒック監視装置１がインターネット中のＡＴＭ回線に接続されているが、ＡＴＭ回線以外の回線に接続されても良く、更には、インターネットに限らず、任意のネットワーク間の回線に接続されても良い。

【００６６】

【発明の効果】以上より、本発明によれば、ネットワーク間の回線上に流れるパケットにできるだけ近い形でトラヒックデータを圧縮して蓄積することができる。従って、高速なインターネット等に対応して、トラヒック監視を長時間運用すること事ができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るトラヒック監視装置の構成例を示す図。

【図２】パケット取得手段の処理手順例を示す図。

【図３】トラヒックデータ蓄積手段の処理手順例を示す図。

【図４】トラヒックデータのフォーマット例を示す図。

【符号の説明】

１　トラヒック監視装置

２　パケット取得モジュール（パケット取得手段）

３　トラヒックデータ蓄積モジュール（トラヒックデータ蓄積手段）

４　統計情報加工モジュール

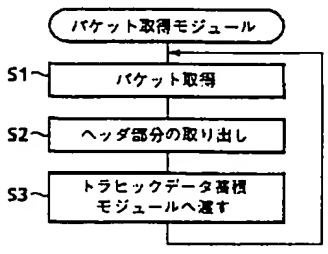
５、６　ＡＴＭ回線

７　トラヒックデータフォーマット

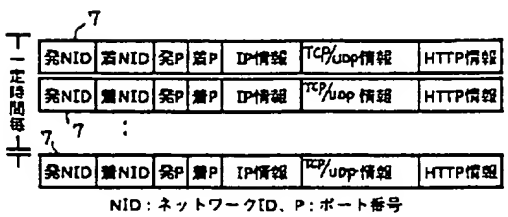
１１、１２　ＡＴＭボード

１３、１４　ＡＴＭルータ又はＡＴＭスイッチ

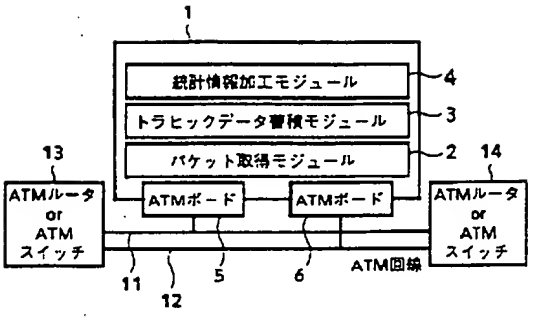
【図２】



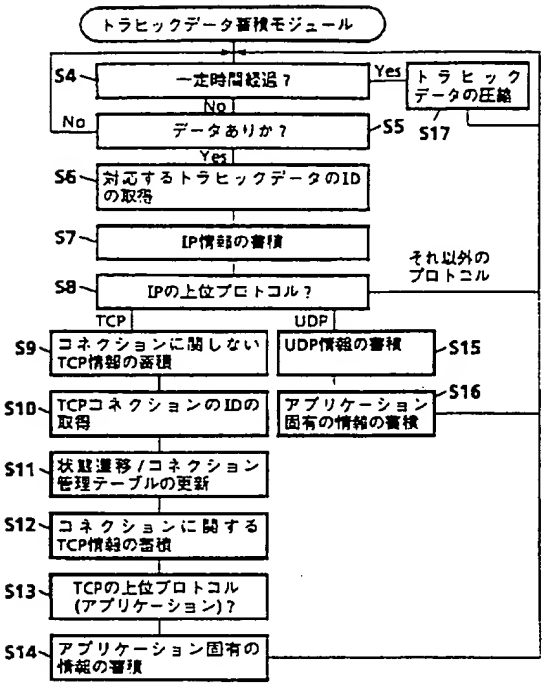
【図４】



【図１】


1
統計情報加工モジュール
4
トラヒックデータ蓄積モジュール
3
パケット取得モジュール
2
13
14
ATMルータ or ATM スイッチ
ATMボード
ATMボード
ATMルータ or ATM スイッチ
11
12
5
6
ATM回線

【図３】


トラヒックデータ蓄積モジュール
S4
一定時間経過？
Yes
トラヒックデータの圧縮
S17
No
No
データありか？
S5
Yes
S6
対応するトラヒックデータのIDの取得
S7
IP情報の蓄積
それ以外のプロトコル
S8
IPの上位プロトコル？
TCP
UDP
S9
コネクションに関しないTCP情報の蓄積
UDP情報の蓄積
S15
S10
TCPコネクションのIDの取得
アプリケーション固有の情報の蓄積
S16
S11
状態遷移/コネクション管理テーブルの更新
S12
コネクションに関するTCP情報の蓄積
S13
TCPの上位プロトコル(アプリケーション)？
S14
アプリケーション固有の情報の蓄積